TECHNISCHE UNIVERSITÄT
IN DER KULTURHAUPTSTADT EUROPAS
CHEMNITZ

MEMS-based Fingerprinting Architecture for Trustworthy Electronics

Schott, Christian[1]; Meinel, Katja[1]; Mayer, Franziska[1]; Gupta, Dhruv[1]; Mittag, Sebastian[1]; Hahn, Susann[1]; Weidlich, Sebastian[1]; Bülz, Daniel[2]; Forke, Roman[2]; Hiller, Karla[1,2]; Kuhn, Harald[1,2]; Heinkel, Ulrich[1]

[1] Technische Universität Chemnitz, Fakultät für Elektrotechnik und Informationstechnik, 09126 Chemnitz

[2]Fraunhofer-Institut für Elektronische Nanosysteme ENAS, 09126 Chemnitz

MOTIVATION

Internet of things (IoT): network of all production systems and their modules → Digitization of process chains

- Increase of process performance, quality and functionality
- Decrease of energy consumption and operation costs

! Modules are vulnerable to manipulation. Possibilities for attack increase with increasing complexity (especially in a global value chain).

Aim

Integration of a Micro-Electro-Mechanical System (MEMS) as physical unclonable function (PUF) in system modules

- Clear identifiability of modules
- Protection against manipulation and unauthorized replacement of original components
- Concepts for integration into architecture and key generation

SYSTEM ARCHITECTURE

Trusted Execution Environment (TEE) (orange)

- RISC-V = representative of interrogating electronics
- Fingerprint device is one entity of TEE

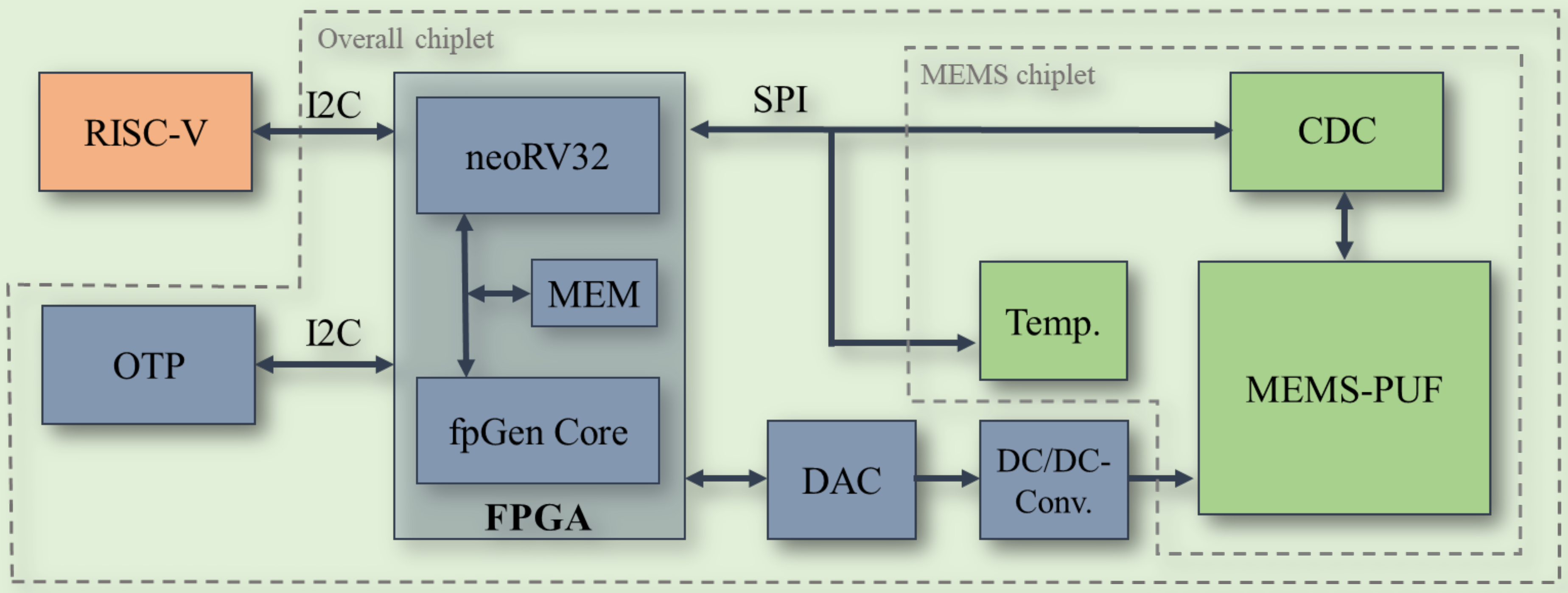
MEMS chiplet (green):

- Specific MEMS component (MEMS-PUF)
- MEMS-related electronics

Fingerprint electronics (blue):

- FPGA and peripherals for controlling and evaluating the MEMS chiplet
- Fingerprint calculation and evaluation with hashed key in OTP

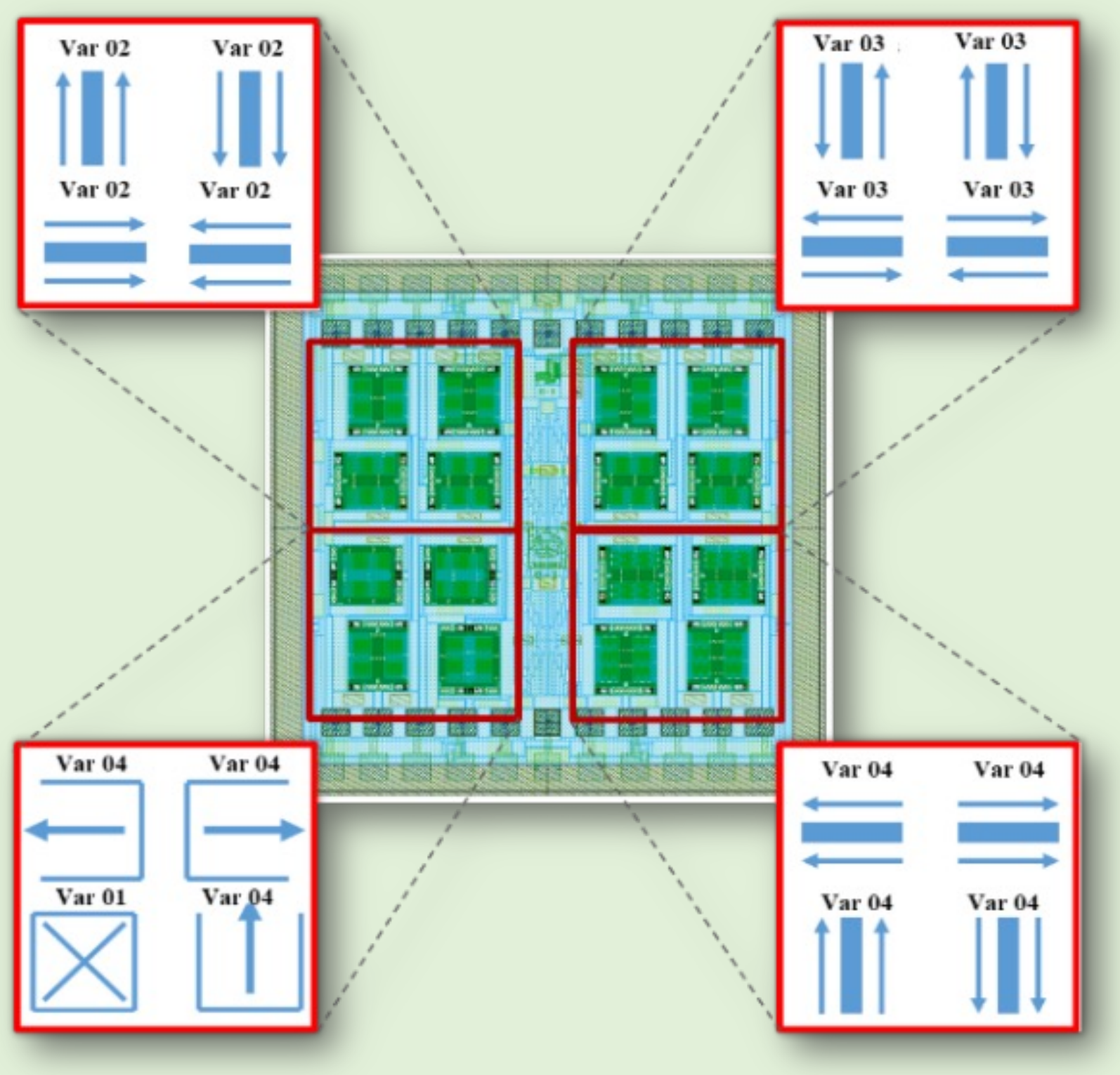
System architecture



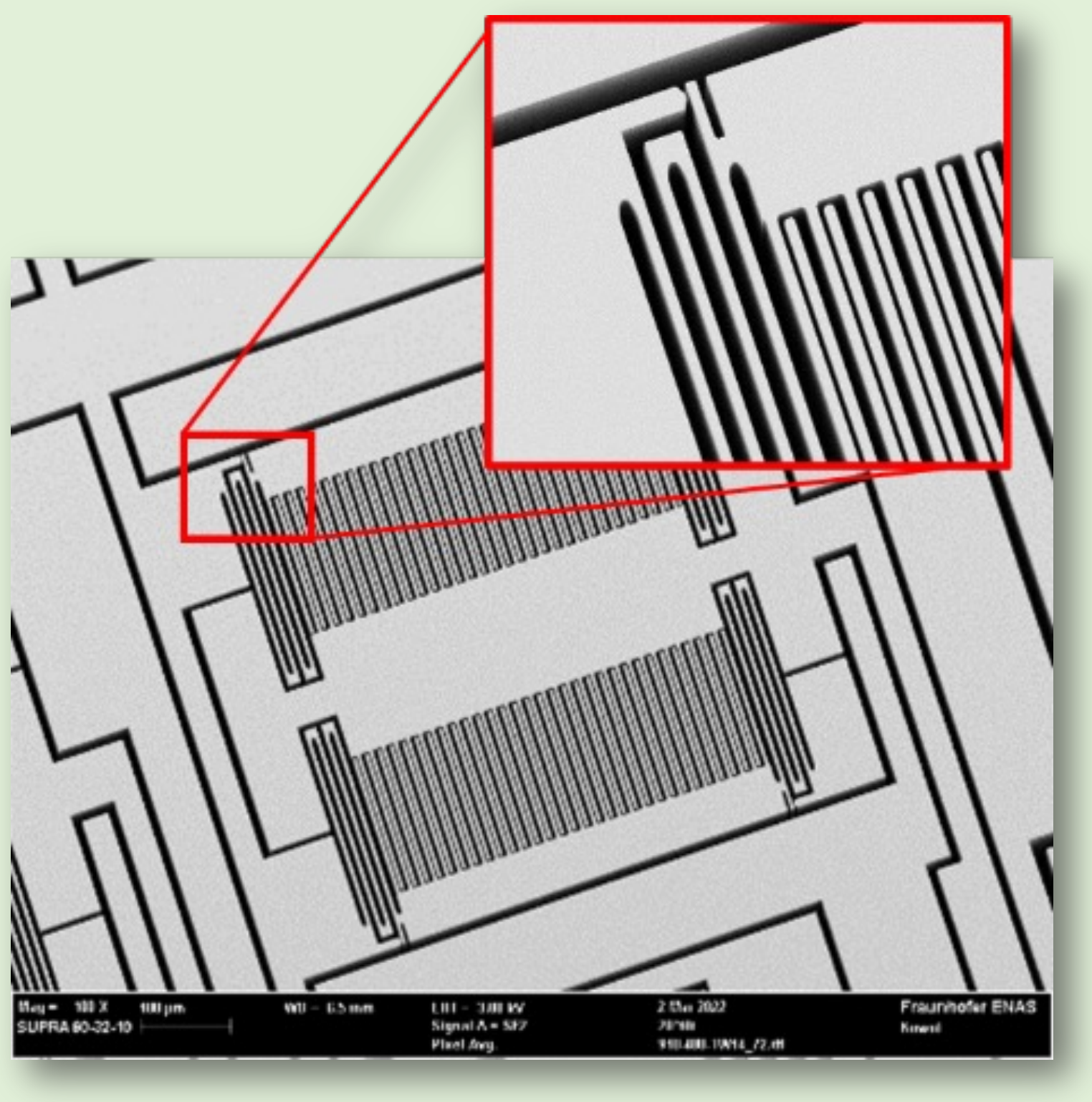
Legend: One time programmble (OTP), Capacitance-to-Digital Converter (CDC), Memory (MEM), Fingerprint generator IP Core (fpGen Core), Field Programmable Gate Array (FPGA), Digital-to-Analog Converter (DAC)

FINGERPRINT MEMS

Design scheme



SEM image of fabricated MEMS



Specific design for PUF application

- Implementation of MEMS, which are inherently prone to scattering/technological tolerances by design
- Focus: Robust design, simple signal detection
  → MEMS varactor array, capacity values used for fingerprinting
  → Forcing of technological spread by special design
  MEMS technology: BDRIE – Bonding and Deep Reactive Ion Etching (Full-Silicon)

MEMS varactor array

- Chip size: 5.1 x 5.1 mm², 16 separate capacities (4 main, 4 sub designs)
- No absolute trends → Basically all designs the same, base capacity identical
- Design variations: Direction, comb geometry, gap spacing, system stiffness

FINGERPRINT ELECTRONICS

neoRV32 microcontroller

- Open source IP-Core, central control unit
- Provides the connection to RISC-V and MEMS-Chiplet
- Readout of CDC and temperature sensor
- Read/configuration of DAC for MEMS driving

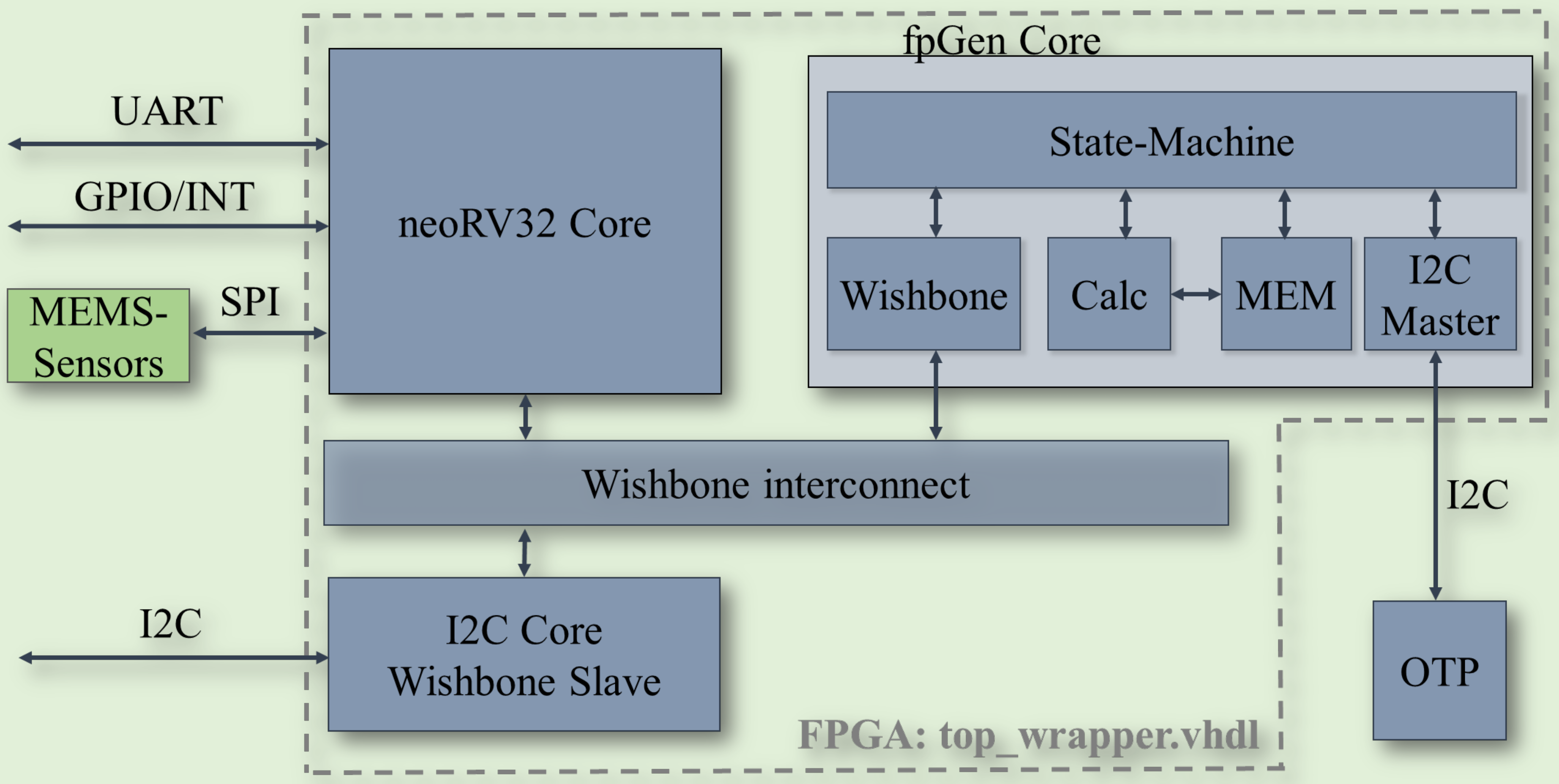
Fingerprint generation Core

- Carries out a cyclic fingerprint generation
- Compares fingerprint with a hashed value in OTP

I2C Core

- Communication with Trusted Execution Environment (RISC-V)

Fingerprint electronics architecture



Bundesministerium
für Bildung
und Forschung

Förderkennzeichen:
16ME0243K - 16ME0254

VE-VIDES

Contact:
Prof. Dr.-Ing. Ulrich Heinkel
Professur Schaltkreis- und Systementwurf
Technische Universität Chemnitz
Reichenhainer Str. 70
09126 Chemnitz

Zentrum für Mikrotechnologien

Fraunhofer
ENAS